n.174
www.hackerjournal.it

WIIMOTE CRACKING

IL MOUSE PERFETTO

INTERCETTAZIONI

SKYPE

SCOPRIAMO LE FALLE

OPEN SOURCE

NIKTO

L'IP SCANNER

SLIPSTREAMING

WINDOWS XP

CREIAMO LA NOSTRA DISTRO

PRIVACY

SIAMO TUTTI CONTROLLATI DAL... CANE

PIRATE BAY

CRONACA DELLA FESTA DEI DEI PIRATI

QUATTORD. ANNO 9 - N° 174 - 16/29 APRILE 2009 - € 2,00

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Diens Alliensis

"Si può resistere ad un'invasione da parte di un esercito ma non ad un'idea il cui momento è giunto".
Alexandre Dumas (padre)

Una data da ricordare, quella del 18 luglio del 387 a.C.: quel giorno i Celti guidati da Brenno travolsero le difese create dai tribuni romani sul fiume Allia, a pochi chilometri da Roma. Festeggiando e saccheggiando, tre giorni dopo, entrarono nella città e nella storia. Alcuni benpensanti avranno certamente fatto un parallelo tra quello scacco militare della ormai ex potenza romana con la festa dei pirati che si è tenuta il 28 e 29 marzo e si è trattato di un parallelo tutt'altro che fuori luogo: i tempi cambiano e molti poteri sono destinati a cadere o, almeno, a trasformarsi.

Siamo in un'Europa soffocata da aziende che mirano a tutelare brevetti hardware e softwa re, qualsiasi musica, qualsiasi video, a riscuotere gabelle ormai anacronistiche, a impedire la libera circolazione di idee, a bloccare la creatività e la conoscenza in nome del profitto. Proprio questa Europa ha assistito alla nascita di un partito pirata che inneggia alla libertà d'espressione e all'abbattimento di queste aziende, che ha avuto un successo insperato e si sta diffondendo sempre più, in contrapposizione ai partiti tradizionali che, ormai, tendono ad assumere una forma assistenziale geriatrica verso le lobby.

L'arrivo dei pirati a Roma, quelli di Pirate Bay ma anche quelli che vivono dello spirito intrinseco dell'Hacker, quelli che non si arrendono, quelli che mal sopportano il clima liberticida creato in nome di leggi antiterrorismo pressoché inutili, non è molto diverso dall'ingresso di Brenno nella stessa città, oltre 2000 anni fa.

Ora staremo a vedere: da movimento sommerso con un proprio linguaggio e propri codici, quasi una nuova carboneria, i pirati sono andati alla conquista della massa, restando fedeli ai loro principi ma uscendo dall'ombra, adattando il loro linguaggio, rendendolo simile a quello delle persone comuni. Persone che, dopotutto, non si sono sentite molto diverse da questi potenziali fuorilegge che puntano il dito verso pachidermici e datati poteri.

La festa si è fatta, altre seguiranno, nuove saranno le proposte, l'attenzione sarà mantenuta. Mai come in questo momento è esistita la possibilità di invadere la società con idee capaci di migliorarla in modo così profondo.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 9 – N.174
16/29 aprile 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

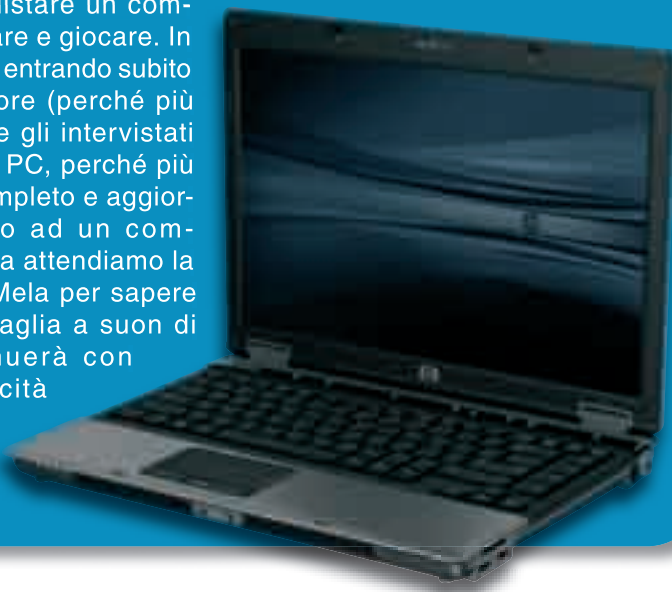
La regione "spiona"

Sulla Rete può capitare un po' di tutto, questo lo sappiamo bene. La maggior parte degli utenti è ignara di questo, e continua a navigare in pace senza preoccuparsene, ma alcuni sono un po' più attenti di altri e, un occhio al browser e uno al firewall, tengono sotto controllo ciò che succede mentre navigano.
Ed è sorprendente sapere che i contatti con altri computer della Rete sono molti di più di quelli che pensiamo, anche solamente visitando una singola pagina Web con il browser.
Prendiamo spunto da una e-mail di un nostro lettore per fare un po' di analisi sul traffico Web. In questo messaggio, Mirko ci comunica che ha il sospetto di essere stato spiato addirittura dalla Regione Toscana, il che è alquanto strano abitando in Lombardia e non avendo nemmeno visitato il sito di detta Regione. L'allarme è arrivato per mezzo di PeerGuardian, un software nato espressamente per proteggere gli utenti delle reti P2P da sguardi curiosi e inopportuni. Questo programma blocca ogni tipo di comunicazione provenga da IP specifici, a prescindere dal protocollo usato. Un'occhiata ai log dei contatti ricevuti è sufficiente per sapere chi ha in qualche modo, intenzionalmente o no, tentato di accedere al nostro computer. Non è un problema risalire da un indirizzo IP al dominio di provenienza, specialmente se nel mezzo non esistono server proxy, e deve essere proprio questo che ha insospettito il nostro Mirko: un IP riportato da PeerGuardian corrispondeva a quello del sito della Regione Toscana. Come è possibile?
Francamente, non crediamo che qualcuno abbia tentato di spiare il PC di Mirko agendo dal server Web della Regione Toscana. Possono esistere diverse spiegazioni, ma la più plausibile è che qualcuno, agendo dalla stessa rete su cui è presente il server Web, si sia collegato a una rete P2P a cui, per coincidenza, era collegato anche il nostro amico. In un caso come questo, sia il server Web sia il computer su cui gira il programma P2P escono pubblicamente con lo stesso IP, che corrisponde a quello del router collegato a Internet. È naturale quindi che un traceroute su quell'IP porti all'indirizzo Web del sito, perché è pubblicamente disponibile nei registri DNS. A nostro avviso, quindi, niente di preoccupante: tutto ciò che raccoglie questo sito è un cookie che identifica univocamente i PC dei suoi visitatori a fini statistici, niente a che vedere con il P2P. Mirko però ha fatto bene a non abbassare la guardia e a insospettirsi: meglio una remora in più che sottovalutare i rischi della Rete.
Nel caso di un vero e proprio attacco verso il nostro computer, lo schema sarebbe ripetitivo, riconoscibile e individuato facilmente da un buon firewall (non certo quello di Windows!): alleniamoci a leggere i log e a riconoscere le situazioni anomale.

GIOVANI CINESI E VIDEOGAME

La lotta del governo cinese contro i giovani affetti da sindrome da videogioco online sembra ottenere i risultati sperati. La percentuale di adolescenti impegnati in questa attività così "pericolosa" è scesa nel corso del 2008 dal 22% al 15%. Il merito è delle misure restrittive imposte sia ai provider che agli Internet point. È bastato limitare a 3 ore il tempo massimo di ogni connessione online e imporre agli Internet Point di identificare tutti gli adolescenti che entravano per giocare. Una censura in più per tutelare i giovani... ma lasciateli "fraggare" in pace!

IL PC FINALMENTE RISPONDE AL MAC!

Le pubblicità comparative proposte da Apple per promuovere i suoi Mac al posto del PC sono state uno degli esempi più divertenti di come si possano evidenziare i difetti di un prodotto avversario con ironia, senza cadere nella diffamazione. Dopo tanti anni in cui il PC ha subito in silenzio gli sfottò del Mac era giunto il momento di affidare alla pubblicità una "risposta ufficiale". È nato quindi lo spot "I'm PC", una specie di reportage in cui alcuni utenti con un budget di 1000 euro dovevano acquistare un computer per lavorare e giocare. In tutti gli spot, pur entrando subito in un Apple Store (perché più trendy) alla fine gli intervistati sceglievano un PC, perché più economico, completo e aggiornabile rispetto ad un computer Apple. Ora attendiamo la risposta della Mela per sapere se questa battaglia a suon di slogan continuerà con la stessa vivacità che ha movimentato gli ultimi spot.

A QUANDO UN WEB 3D?

In futuro le pagine Web potrebbero non esistere più, sostituite da spazi virtuali 3D. Per ora è poco più che fantascienza, anticipata da pochi esperimenti di scarso successo, ma grazie alla collaborazione tra Mozilla, popolare software house che ha creato Firefox e Thunderbird, e Khronos Group, specializzato nella modellazione 3D, forse non ci vorrà molto per vedere le prime pagine 3D su Internet. Per realizzare questo nuovo sistema di interazione con il Web, le due aziende hanno pensato di affidarsi alle API OpenGL ES 2.0 ideali per essere integrate nel linguaggio javascript alla base della programmazione delle pagine Internet. Se il progetto dovesse andare in porto si tratterebbe di una svolta epocale nell'interazione con il Web che aprirebbe nuovi scenari e nuovi servizi fruibili per chiunque direttamente su Internet, come ad esempio la possibilità di organizzare le informazioni tridimensionalmente per migliorarne la reperibilità e ridurre il numero di clic a link e pagine secondarie.

HOT NEWS

TI GUIDO OVUNQUE MA GUARDA DOVE VAI!

A volte fidarsi troppo del navigatore satellitare può costare davvero caro. È il caso di un automobilista inglese, tale R. Jones, che ha deciso di ignorare i numerosi segnali sulla strada, incluse quelle asfaltate, per seguire fedelmente la rotta tracciata dal suo inseparabile navigatore che lo ha portato... a pochi centimetri dalla morte.
L'auto guidata dal signor Jones, una BMW, aveva imboccato una stradina di montagna che portava direttamente ad un profondo e pericoloso dirupo. Ovviamente non segnalato sulla mappa del navigatore. Solo la rete di protezione ha salvato l'incauto automobilista da morte certa. Non è la prima volta che cose simili accadono, come quel caso di un fiume indiano in cui più di un automobile si è impantanata proprio a causa del Tom Tom... Insomma finché non inventeranno un navigatore a prova di idiota e con mappe super aggiornate, magari, è meglio stare attenti.

SOLDI PER CHI SVILUPPA "OPEN SOURCE"

L'idea è grandiosa e unisce la virtù dei benefattori con la logica capitalistica del profitto. Stiamo parlando della "banca per lo sviluppo open source" un istituto di credito nato per finanziare i progetti informatici più ambiziosi. Ad avere l'idea sono stati due signori americani, Justin Huynh e Matt Stack, che hanno pensato ad un sistema per remunerare i progetti più interessanti, rigorosamente open source, facendoli finanziare da altri programmatori che hanno già raggiunto il successo professionale ed economico. Molto spesso infatti è assai difficile per i programmatori indipendenti trovare il denaro necessario per registrare il proprio brevetto e renderlo disponibile, soprattutto se si tratta di hardware e software open source, per cui spesso gratuito. Anche se non sappiamo ancora quanto successo avrà l'idea dei due programmatori, perché "creare" una banca non è affatto semplice, apprezziamo comunque il tentativo di abbattere le logiche del mercato e puntare sulle idee rivoluzionarie.

BANCOMAT CRACCATI

Tranquilli... è successo in Russia. Mentre da noi i criminali tentano ancora di bypassare il codice bancomat con lettori e telecamerine per riprendere i codici, in Russia sono avanti anni luce. Alcuni ATM Diebold (famoso produttore mondiale) infatti sono stati hacherati con un particolare software che ha permesso a criminali informatici di inserire all'interno del sistema operativo un trojan capace di registrare e inviare in remoto tutti i log delle operazioni effettuate dagli ignari utenti allo sportello. La novità di questo attacco sta nel fatto che gli sportelli bancomat non sono stati manomessi dall'esterno, come capita oggi, ma dall'interno, tramite software. Chiaramente dalle indagini, ancora in corso, è emerso che qualcuno all'interno della banca deve aver "agevolato" l'ingresso degli hacker nel sistema, ma c'è da dire che non si era mai visto un virus progettato appositamente per girare su un bancomat.

UK, 25 archivi su 100 sono illegali

Tutti i dati che inseriamo in vari forum, siti e altro ancora, vengono spesso ceduti a società che si occupano di conservarli e utilizzarli per elaborare nuove strategie di mercato. Il problema però è che a volte non siamo noi a fornire questi dati, ma piuttosto le società a "rubarli" con qualche stratagemma più o meno lecito. Nella vecchia Inghilterra questo fenomeno è ormai diffusissimo tanto che, in seguito ad un'indagine del governo di Londra per stabilire la "legalità" di questi database con le nostre informazioni, ben 11 su 46 società prese in esame si sono rivelate completamente illegali. In molti database non si trovavano solo informazioni su gusti e preferenze ma anche cartelle cliniche, documenti personali e altri dati completamente lesivi del diritto alla privacy.

LADRI DI IPOD! 9000 ALL'ANNO...

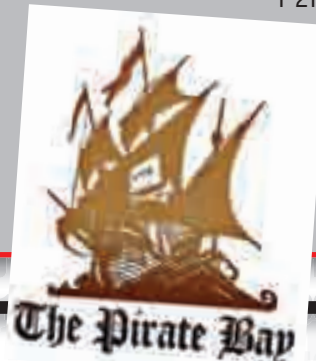
La criminalità non ha confini e molte volte leggiamo di furti di tecnologia nei negozi o nei supermercati... di solito si tratta di piccole cose, spesso scoperte al volo tramite i sistemi di sicurezza. Ma in questo caso abbiamo davanti un vero genio della truffa! Il signor Nicholas Arthur Woodhams è stato arrestato nel Michigan per aver "sottratto e venduto" oltre 9000 iPod con uno stratagemma molto ingegnoso. Woodhams infatti possiede un piccolo centro assistenza Apple che, come tutti i centri di questo tipo segue la politica della "sostituzione rapida" dei prodotti difettosi. In pratica, una volta segnalato il numero di serie del prodotto, Apple invia al negozio un nuovo iPod molto prima che quello difettoso torni "alla base". Arthur aveva trovato un sistema per generare falsi numeri di serie degli iPod, facendosi inviare da marzo 2007 a novembre 2008 un numero impressionante di iPod che rivendeva a prezzi inferiori a quello imposto del 20-30%. Purtroppo, come del resto c'era da aspettarsi, Apple si è insospettita quando non ha visto tornare i 9000 iPod difettosi del negozio di Woodhams. Ulteriori indagini hanno portato all'arresto del "fenomenale" truffatore. Chissà se Apple ha regalato un iPod al malcapitato per passare meglio i suoi giorni in galera...

IL PRIMO WORM PER I ROUTER

Passare l'antivirus sul PC probabilmente tra qualche anno non basterà più, ma occorrerà proteggere anche altri dispositivi come ad esempio il router. Questi "ponti" che ci collegano ad internet infatti sono diventati sempre più evoluti, tanto da montare ormai veri e propri sistemi operativi. PsyB0t è il primo esempio di worm in grado di attaccare direttamente il router a cui è collegato il nostro PC. Grazie al suo elaborato codice di programmazioe PsyB0t è in grado di "analizzare" i pacchetti inviati e ricevuti dalla nostra connessione a Internet e di trasformare il nostro router in una potente arma per lanciare attacchi di Denial of Service verso altri siti Web, Provider, e servizi. Ricordiamo che il Denial of Service non è altro che il tentativo, molto spesso fruttuso, di far collegare milioni di computer infetti allo stesso server in modo tale da saturarne la banda in ingresso e uscita, di fatto, bloccandolo completamente.

UE ATTACCA, PIRATE BAY RISPONDE

Tra le iniziative studiate dai governi europei per bloccare l'utilizzo del P2P per scambiarsi dati protetti da copyright, c'è l'introduzione per i provider, dell'obbligo di tracciare e segnalare il tipo di attività di ogni singolo utente nel caso di utilizzo della tecnologia P2P. In pratica, chiunque provi a scaricare un file tramite torrent, potrebbe venire registrato e successivamente multato. Per fortuna Pirate Bay è intervenuta tempestivamente ad annullare il tentativo dell'UE rilasciando un software in grado di "nascondere" l'identità di chi scarica file dal suo portale. Il software si chiama iPredator ed in pratica stabilisce una VPN tra il nostro computer e un server che si trova in paesi non europei (prevalentemente dell'Est): tutte le operazioni di download che effettueremo, passeranno quindi dal server remoto, impedendo ai provider di individuare il flusso P2P (che non avverrà direttamente sul nostro PC) e lasciandoci "puliti" con i nostri bravi film e musica scaricati. È proprio vero: fatta la legge, trovato l'hacking... pardon, l'inganno!

HOT NEWS

PHISHING "MIRATO"

Nelle foto si chiama "geotagging", ovvero la possibilità di aggiungere all'immagine anche le coordinate geografiche di dove è stata scattata,

tramite un sistema GPS o una triangolazione radio. Ebbene, oggi è possibile "geotaggare" anche le mail di phishing. Alcuni pirati informatici hanno infatti messo a punto un sistema di creazione automatica di mail di phishing partendo dall'indirizzo IP dei destinatari del messaggio. Analizzando infatti l'indirizzo IP del server a cui le email verranno inviate, questo elaborato software è in grado di scegliere automaticamente la lingua del messaggio e il tipo di ente, banca, sito più adatto per imbrogliare gli utenti.

APPLE, REGINA DI CLONI

Che i prodotti di Apple siano tra i più "clonati" del mondo, soprattutto dai cinesi, lo sanno tutti, ma che adesso la Mela chiamasse in causa anche chi clona il nome o parte del nome dei suoi prodotti è davvero troppo. Pivotal, azienda specializzata in accessori per Mac si è vista chiamare in causa da Apple per aver messo in commercio un particolare supporto per iPod e iPhone chiamato, incredibile, Podium. Secondo i legali di Steve Jobs, infatti, la parola Pod contenuta nel nome è di esclusiva proprietà di Apple e per questo Pivotal dovrebbe pagare i danni legati alla mancata richiesta di sfruttamento del marchio registrato. Beh, pensando che la parola "podium" viene dal latino e vuol dire "piede", sono previste cause contro Virgilio, Cicerone, Seneca, Orazio o Catullo?

RICARICHE NATURALI

In futuro potremmo ricaricare le batterie del cellulare prendendo energia cinetica dallo scorrere del nostro sangue o da tutti quei fenomeni naturali come il vento, il sole o anche la caduta delle foglie. Un gruppo di ricercatori giapponesi infatti sta mettendo a punto un sistema di ricarica in grado di raccogliere energia dalla conversione di vibrazioni a bassa frequenza, grazie a dei particolari nanofili all'ossido di zinco che conducono elettricità. Se questa ricerca otterrà i risultati sperati, presto il cellulare scarico nel bel mezzo di una scampagnata sarà solo un lontano ricordo.

VIOLENZE IN TIBET, PECHINO CENSURA YOUTUBE

Evviva il grande popolo cinese! Il governo più "simpatico" del mondo ha deciso di censurare, in via del tutto eccezionale ovviamente, i video su Youtube che riprendevano diversi atti di violenza da parte della polizia e dell'esercito cinese ai danni di "normali" cittadini tibetani tra cui monaci, donne e bambini.

Il democratico Paese, con cui fa affari mezzo mondo, ha ritenuto poco adatti alla sensibilità dei suoi cittadini i contenuti dei video e li ha fatti rimuovere tutti, in men che non si dica, dal portale video più famoso del pianeta. Vergogna per la Cina? No, una vergogna per tutti quei Paesi occidentali, Italia inclusa, che pretendono di essere portatori di democrazia e poi si piegano docilmente alla dittatura cinese per guadagnarsi le simpatie del "mercante" asiatico e risparmiare sui costi di produzione.

Illustrazione di Daniele Festa

"LA FESTA DEI PIRATI"

Ovvero, quando un'intera generazione dice sì al P2P

Guardare da dietro il mondo è sempre una prospettiva interessante: angolazioni, punti di vista, scorci e inquadrature capaci di sovvertire le facciate. La potremmo definire anche un'attitudine - analogica e digitale - quella di chi alle porte d'ingresso principali predilige le entrate secondarie, gli accessi nascosti, le strade minori, i percorsi a ritroso e che spesso coincide con un istinto irrefrenabile a smontare, invertire, decostruire le strutture e i sistemi.
Fatto sta che i pirati (svedesi), quelli che abitano la Baia digitale più famosa al mondo, a Roma il 28 marzo per la festa che li celebra, alla fine entrano dal retro. E per di più quello di una chiesa.

:: Location

Se la facciata svolge le funzioni religiose dell'edificio, il suo retro ne ospita il lato tutto laico, pagano, commerciale. Si tratta del Teatro delle Arti, da poco inaugurato dopo la ristrutturazione. Siamo a Piazza Triora, nel cuore di Garbatella, quartiere simbolo dell'edilizia popolare fascista, della memoria partigiana, della vita notturna romana e il Teatro è una vera chicca per la Festa dei Pirati: sala da 300 posti, piccolo anfiteatro in pietra, è un antro completamente nero, scavato in un seminterrato dai soffitti altissimi.

:: Genesi

Recentemente edito da Cooper, esce "La Baia dei Pirati. Assalto al copyright". Il libro, scritto da Luca Neri dopo l'oscuramento dei server italiani di Pirate Bay, è il catalizzatore dell'evento. È così che pirati svedesi raccontati dal libro "calano a Roma", per confrontarsi con realtà italiane affini, alcune delle

Corridoio del Teatro: banchetti espositivi si alcune associazioni promotrici che spiccano sulle pareti nere.

quali, come LOOP, Frontiere Digitali, Linux-Club Italia, Scambio Etico, Partito Pirata, TnT Village, Free Hardware Foundation, FPML RomaeuropaFAKEFactory, Art is Open Source, LPM, FLxER, si attivano per offrire ospitalità e organizzare attrezzare lo spazio.

:: Programma

La mattina si apre col mini corso di p2p per principianti a cura Franco Noè e Andrea Tavi, due studenti di Scienze della Comunicazione deliziosi nell'ammettere il loro imbarazzo: "il pubblico in sala sapeva più di noi!". Seguono gli interventi del Linux Club, sull'esigenza di "un nodo fisico" per la rete come fattore di aggregazione territoriale, di TnT Village e dei legali italiani (Gallus e Micozzi) che difendono Pirate Bay dopo l'oscuramento: il processo è in corso. Nel pomeriggio i lavori riprendono con l'atteso incontro dedicato a Magnus Eriksson e Johan Allgoth, i "veri" pirati della Baia, protagonisti della festa e di un piccolo detournamento. Lo speach si tiene infatti nel REFF.theatre, spazio installativo/performativo allestito da Art is Opensource: ad attirarli, come ci spiegano, un linguaggio comune e la volontà di stabilire un contatto intimo con il pubblico. Ci riescono perfettamente: l'attenzione è alta, piovono domande e curiosità sul caso Svezia. Ne risulta un quadro dove una generazione di giovani svedesi si è riconosciuta nella difesa dei nuovi commons digitali: il P2P a quanto pare dilaga nelle liste studentesche. Nella sala grande gli interventi si susseguono implacabili con la moderazione di Arturo di Corinto (FHF)e Athos Gualazzi (P2P Italia). Tre i momenti caldi, che alzano la tensione del pubblico. Il primo è la presentazione di Luca Neri dove esplode la contraddizione del progetto editoriale: un libro sul no-copyright viene rilasciato con licenza all rights reserved. È un esponente dei LUG ad accendere la miccia: mentre Neri invita a piratare il suo libro, si dice già al lavoro per trovare un accordo col suo editore. Il secondo è la relazione Carlo Blengino, avvocato responsabile del caso Peppermint, che puntualizza come la attuale legislazione sul diritto d'autore (storicamente pre-digitale) sia incompatibile con i diritti di privacy sanciti dalla costituzione. In sostanza, chi voglia "seguire" un contenuto protetto per verificare l'infrazione di copyright, deve rovistare nelle nostre comunicazioni personali, per le quali l'ordinamento prevede procedure specifiche. Un aporia che, senza arrivare alla società del controllo di Orwell, sintetizza elementi di conflitto reali e inquietanti sulla definizione dei diritti personali. Il terzo è invece l'intervento di Erik Josefsson che, insieme a Paolo Brini (attivista), propone una densa

Magnus Eriksson e Johan Allgoth nel REFF.theater mentre raccontano al pubblico la storia di The Pirate Bay.

Da sinistra, Paolo Brini e Erik Josefsson. Proiettato sullo schermo campeggia il logo del progetto Patent Bay.

relazione sul Telecom Package. L'oscuro "Pacchetto", in valutazione presso la Commissione Europea, contiene articoli che autorizzerebbero la discriminazione sui contenuti che viaggiano online, aprendo la prospettiva di una rete frammentata e isolata in sottoreti. Josefsson ha coordinato la campagna di sensibilizzazione e l'azione di lobbing sui parlamentari europei, con un risultato: i documenti del tavolo di contrattazione, prima segreti, sono ora consultabili. Josefsson è inoltre ideatore del progetto "Patent Bay", estensione di Pirate Bay ai brevetti. Pare infatti che negli uffici Bruxelles si inizi parlare di "Patent Warming", ovvero l'insostenibile inquinamento da brevetto.

:: Arrivederci!

Forse è mancata l'anima del raduno, ma una cosa è certa, l'evento è riuscito nell'intento di imporsi e bucare i media. I pirati e il loro mondo che tendenzialmente vive e si produce in rete o in spazi interstiziali del tessuto urbano hanno calamitato l'attenzione di TG e testate nazionali. Peraltro in modo giocoso, positivo e con un messaggio riconoscibile: pirati lo siamo un po' tutti. E poter affermare questi concetti pubblicamente, su canali mainstream, non è poco nel clima politico italiano che fa presagire tempi di dure restrizioni per le libertà in Internet e di chi la abita.

Penelope.Di.Pixel

DURI A MORIRE

Scopriamo un ambiente di sviluppo non nuovissimo ma ancora oggi molto usato

La vita del software al giorno d'oggi è piuttosto breve: se prendiamo in esame una singola release di un programma, probabilmente la vedremo sul mercato al massimo per un annetto o giù di lì, difficilmente di più. A volte invece, pur avendo a disposizione valide alternative, certi software riescono a sopravvivere nel tempo grazie alle comunità che li adottano, o anche semplicemente perché sono talmente utili o semplici da usare che si continua a usarli "per inerzia". È un po' quello che è successo a Dev-C++: tra gli appassionati, è ancora probabilmente l'IDE per creare i propri programmi più usati da hobbysti e appassionati di tutto il mondo. Innanzitutto è gratuito e semplice da usare, e questo aiuta. Inoltre, nel corso del tempo sono stati creati numerosi pacchetti di librerie e di codice facilmente importabili sul proprio sistema di sviluppo basato su Dev-C++, che vengono tuttora aggiornati (al contrario del programma, che ormai dal 2005 non vede più nuove release).

:: Come ottenerlo

Dev-C++ è liberamente scaricabile dal sito ufficiale http://www.bloodshed.net. Esplorando le pagine del sito scopriremo anche altre risorse che possono tornare utili agli appassionati di programmazione. Per esempio un'utility per creare procedure di installazione per i propri programmi (setup.zip) o Dev-Pascal, un IDE simile a Dev-C++ ma che usa il compilatore Pascal gratuito Free Pascal. L'ultima release disponibile è la 5.0 beta 9.2, ospitata da Source Forge insieme ai sorgenti Delphi. Malgrado si tratti di una versione beta, è molto stabile e matura, e si può usare in ogni tipo di progetto. L'installazione avviene mediante una normale procedura di setup e non comporta alcuna difficoltà. Al termine, ha luogo una breve configurazione iniziale guidata, in cui potremo scegliere anche

La home page di Dev-C++: anche il sito è fermo al 2005 ma il software è ancora ampiamente usato dagli appassionati.

la lingua per i menu, per i quali è disponibile anche l'italiano. A parte la lingua, le altre opzioni possono essere lasciate sui valori predefiniti, che sono impostati per un uso abbastanza costante: per esempio potremmo trarre vantaggio dal browser di oggetti, che ci aiuta a trovare le definizioni delle nostre funzioni in caso di programmi abbastanza ampi. A questo punto siamo pronti per iniziare a usare il nostro nuovo IDE per sviluppare in C++. Ci basta creare un nuovo progetto (File → New → Project, se abbiamo mantenuto l'inglese) e cominciare a scrivere il codice.

Possiamo creare diversi tipi di applicazione, grafica o a linea di comando, e anche librerie di vario genere: se installiamo le librerie aggiuntive avremo a disposizione altri tipi di applicazioni.

:: Il repository

La cosa più interessante di Dev-C++ è la disponibilità di numerose librerie organizzate in pacchetti di installazione (con un procedimento che ricorda molto i pacchetti RPM di Linux) che possono essere liberamente scaricati e installati. La procedura avviene attraverso un modulo interno al programma, che si appoggia a un repository online per recuperare i pacchetti desiderati e per installarli automaticamente. In teoria, la stessa procedura permette di aggiornare automaticamente lo stesso Dev-C++, ma dato che lo sviluppo è ormai fermo da anni al momento è utile solo per recuperare i pacchetti delle librerie. Per accedere a questa funzione basta aprire il menu Tools e selezionare Check for Updates/Packages. Da notare che il sito PlanetMirror.com, che appare come impostazione predefinita, non è più attivo da tempo, pertanto occorre scegliere la seconda voce del menu a tendina (devpacks.org Community Devpacks) e fare clic su Check for updates per ottenere la lista dei pacchetti disponibili. Eventualmente, possiamo scegliere di visualizzare solo i pacchetti appartenenti a una determinata categoria, scegliendola tra quelle mostrate nel menu a tendina Groups. Fatto questo, non ci rimane altro da fare che selezionare quelli che ci interessano e fare clic su Download selected. Al termine di ogni download viene avviata automaticamente la procedura di installazione, dopo la quale la libreria è disponibile per i nostri programmi.
È molto utile anche il supporto per le dipendenze: se una libreria che vogliamo installare si basa su un'altra che ancora non abbiamo sul nostro computer, il sistema ci avvisa e annulla l'installazione, così potremo scaricare la libreria di supporto e installarla prima di quella che ci serve. Attraverso un altro importante strumento, il Package Manager, possiamo gestire i pacchetti installati sul nostro PC.
Questo strumento ci aiuta anche nell'installazione di pacchetti eventualmente trovati sul Web ma non disponibili sul repository ufficiale (anch'esso purtroppo aggiornato raramente). I pacchetti sono archivi compressi contenenti tutti i file necessari per la libreria (sorgenti, header, binari, guide e quant'altro) che presentano estensione .devpak. Scaricato un pacchetto, avviamo il Package Manager (Tools → Package Manager), facciamo clic su Install e sfogliamo il disco per individuare il pacchetto. Al resto ci pensa Dev-C++.

Il recupero e l'installazione automatica dei pacchetti delle librerie avviene per mezzo di un apposito strumento integrato nell'IDE.

Il Package Manager di Dev-C++ aiuta nella gestione dei devpak, i pacchetti di installazione delle librerie di supporto disponibili in Rete.

Nessuno è al sicuro

Molti pensano che Skype non sia davvero così al riparo da intercettazioni telefoniche

Skype è attualmente il più famoso software di VoIP disponibile, con oltre 405 milioni di utenti in tutto il mondo che lo utilizzano quotidianamente per far chiamate, videoconferenze, scambio di file e chat. Realizzato dallo svedese Niklas Zennström e dal tedesco Janus Friis (fondatori anche di Kazaa e di Joost [ex. Venice Project]) è stato venduto nel settembre 2005 al colosso di eBay per la spaventosa cifra di 2,6 miliardi di dollari.

:: Intercettazioni

Nell'ultimo periodo è salito agli onori della cronaca grazie ad alcune dichiarazioni del nostro Ministro degli Interni riguardo all'impossibilità, da parte delle forze dell'ordine, di intercettare questo tipo di chiamate. Secondo il ministero e la procura antimafia i criminali si sarebbero infatti "evoluti" effettuando telefonate tramite sistemi VoIP come Skype che prevedono la cifratura delle chiamate. Il Ministro non ha escluso la possibilità di chiedere l'intervento dell'Unione Europea per ottenere le "chiavi di Skype" (la sede legale di Skype è infatti in Lussemburgo). Ma è vero che non è possibile intercettare questo tipo di chiamate?

:: Sistema

Skype è un software proprietario (il codice sorgente non viene quindi distribuito) che utilizza un sistema di connessioni decentralizzato simile ad un qualsiasi software P2P. Esso sfrutta direttamente gli utenti collegati al network nominandoli, tramite particolari algoritmi, "nodi" o "super-nodi" della rete. Non esistono infatti dei server centrali dove vengono instradate le connessioni effettuate, tranne che per l'utilizzo del servizio "SkypeOUT", vedi **Figura 1**.

:: Cifratura

Skype utilizza diversi collaudati sistemi di cifratura: durante la registrazione di un nuovo utente, il client genera una chiave RSA asimmetrica univoca che viene inviata, assieme all'username e alla password scelti, tramite una connessione criptata AES (Advanced Encryption Standard, anche nota come cifratura Rijndael, utilizzata anche da enti governativi degli Stati Uniti per proteggere informazioni riservate) al server centrale di login. Questa chiave viene utilizzata dal server per certificare il client

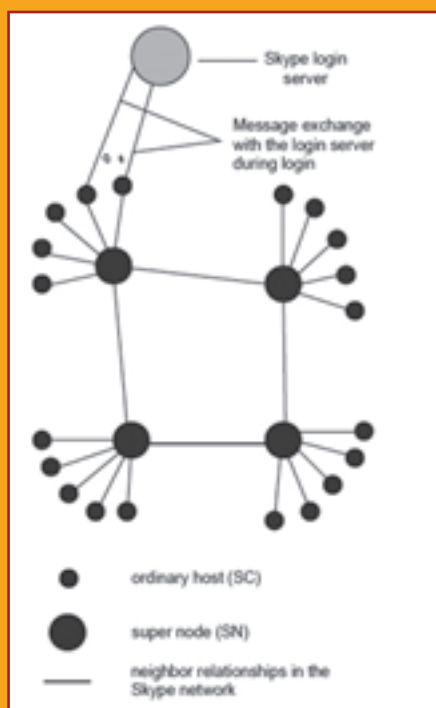



Figura 1. La struttura del network.

durante la fase di login, come descritto in **Figura 2**.

Quando invece viene creata una chiamata tra due o più utenti, la sessione viene inizializzata tramite lo scambio di una 256-bit session key e lo schema di collegamento può essere definito come un semplice sistema di architettura P2P, vedi **Figura 3**.
Giusto per capire quanto sia "imponente" la cifratura AES, l'NSA americana (National Security Agency) dà come indicazione ai propri uffici di cifrare i documenti classificati a livello "SECRET" con una chiave a 128bit, mentre per i documenti classificati come "TOP SECRET" consiglia l'utilizzo di una chiave di lunghezza compresa tra 192 bit e 256 bit.

Considerando che la chiave RSA per negoziare le chiavi simmetriche AES ha una lunghezza compresa tra 1536 a 2048 bit e che come detto precedentemente le chiavi AES sono lunghe 256bit possiamo proprio dire che il sistema di Skype (almeno per lo stato attuale delle conoscenze sulla crittografia e sulla potenza di calcolo dei pc) è a prova di "bomba".

:: Impossible is nothing

Ma allora è veramente impossibile intercettare una conversazione? I criminali riusciranno a farla franca? La risposta è NO.
In tanti infatti ipotizzano che Skype abbia inserito appositamente all'interno del codice sorgente una backdoor che permetta di sniffare il traffico prima che venga cifrato dagli algoritmi sopra descritti. Basterebbe infatti inserirsi all'interno del sistema e "ascoltare" le conversazioni prima che esse vengano cifrate e trasmesse nel network. Ma come facciamo noi utenti a sapere se Skype è sicuro o meno? Il problema è che non lo si può sapere con certezza. Il codice infatti, essendo proprietario, non viene liberamente distribuito e il sospetto che Skype abbia inserito qualche features nascosta di questo tipo è venuta a più di un'utente. Diversi studi di reverse engineering hanno evidenziato come, analizzando il traffico in uscita da Skype, ci siano diversi "byte" quantomeno sospetti.
Cosa che fa ancora più paura al riguar-

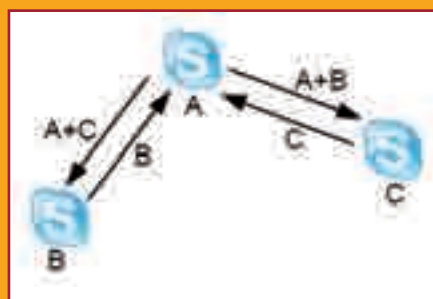



Figura 3. L'architettura P2P.

do è che Skype utilizza di default per la connessione alla rete la porta 80. Questa porta viene utilizzata anche per le connessioni HTTP e, per questo motivo, è la meno controllata da Firewall e software di sicurezza. Una falla in Skype (voluta o meno) potrebbe quindi provocare effetti catastrofici: oltre 405 milioni di utenti sarebbero facilmente vulnerabili ad un qualsiasi tipo di attacco senza che firewall o software del sistema se ne possano accorgere.
La facilità con cui Skype ha poi deciso di collaborare con la polizia nelle intercettazioni, in seguito agli appelli dell' EUROJUST (l'organismo europeo che coordina le indagini in materia di criminalità informatica), fa presagire che si fosse già preparata ad una richiesta di questo tipo. Che soluzioni ci sono a riguardo? La privacy degli utenti è destinata a morire (ma è mai esistita?) in nome della sicurezza nazionale? In attesa di saperne di più, come sempre, accendiamo il cervello e… prudenza, il nemico ti ascolta.

Figura 2. Algoritmo di login.

Juice

APPROFONDIMENTI

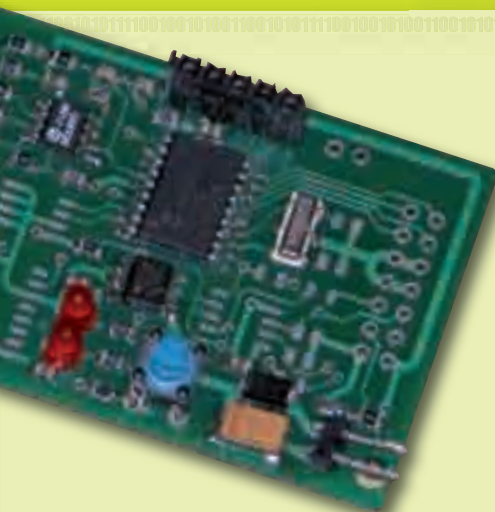
http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf
http://www1.cs.columbia.edu/~salman/skype/OSI_Skype6.pdf
http://www.ossir.org/windows/supports/2005/2005-11-07/EADS-CCR_Fabrice_Skype.pdf

CYBERBESTIE

Tutti i cani hanno un chip per l'identificazione. E se servisse per identificare il padrone?

È dal 1991 che la legge obbliga alla dichiarazione di possesso e alla registrazione dei cani presso l'anagrafe canina. In origine questa registrazione comportava l'assegnamento al cane di un codice univoco che veniva tatuato ma il sistema era tutt'altro che funzionale: dopo qualche anno il tatuaggio, a causa del veloce ricambio di pelo, diventava illeggibile. Così si è passati a un sistema elettronico: un minuscolo chip racchiuso in una capsula di materiale biocompatibile lunga 11 mm e di 2,1 mm di diametro. Viene inserito sottopelle grazie a un semplice ago e ha dato vantaggi immediati: applicazione indolore, durata nel tempo, possibilità di controlli tramite scanner, senza dover operare a lungo e manualmente con l'animale. Tutta un'altra vita rispetto al vetusto e desueto tatuaggio.

:: Un numero importante

Proprio il fatto che sia un componente elettronico, manco a dirlo, è l'aspetto che ci interessa. Tecnicamente, il microchip è un trasponder passivo che segnala agli scanner dedicati un codice identificativo composto da 15 numeri. Il codice è parzialmente parlante ed è composto dall'indicazione della nazione in cui è stato taggato il cane, un numero corrispondente al produttore del microchip e da un numero che identifica realmente l'animale. Viste le dimensioni e la scarsa utilità delle informazioni che trasmette, non c'è interesse nell'hackerare un dispositivo del genere. Ad ogni codice corrisponde un record del database regionale che permette di risalire al padrone del cane e ad altre informazioni utili. Proprio questo, però, è l'anello debole di tutto il sistema. In Italia, il database è regionale e significa che un cane con chip abbandonato in una regione diversa da quella di residenza è equivalente di un cane senza microchip. Anche se questo aspetto sarebbe un ottimo spunto per un manuale su come non si costruiscono sistemi informativi, ha comunque un interesse limitato

Questo modulo, chiamato XP410, è un lettore di transponder con antenna integrata. È molto piccolo e non legge informazioni da grande distanza ma può essere ulteriormente migliorato.

per quanto riguarda il nostro tema. La vera rivoluzione si ottiene unendo un po' di social engineering, queste notizie sui microchip canini e la notizia, uscita qualche tempo fa, che un ricercatore è riuscito a costruire un sistema tracciante per chip RFID a lunga distanza.

:: Seguire la bestia

L'esperimento di intercettazione, di cui abbiamo parlato nel numero 171, è stato svolto realizzando un sistema di ricezione occultato in un'auto, con parti acquistate normalmente sul mercato e mezzi economici comunque limitati. Malgrado le premesse, i risultati hanno permesso di tracciare chip RFID distanti qualche metro: una distanza decisamente più elevata rispetto ai pochi cm a cui dovrebbe funzionare questa tecnologia per poterci assicurare un po' di privacy. D'altra parte il ricercatore che l'ha condotto ha affermato e dimostrato che gli stessi mezzi possono essere utilizzati per intercettazioni a distanze maggiori, fino a due miglia, pari a 3 Km, metro più, metro meno. A questo occorre aggiungere che la velocità di trasmissione dei segnali radio e i tempi di reazione dei chip sono misurabili in modo estremamente preciso: basta pensare al sistema di triangolazione dei segnali GPS, basato su scale temporali infinitesimali. Unendo i due punti di vista possiamo affermare che un sistema di tracking dei chip RFID in uno spazio 3D di circa 3 Km di lato può essere realizzato grazie a un sistema di triangolazione basato su 3 stazioni di intercettazione.Il problema riguarderà certamente un uso futuro dei chip RFID ma allo stato attuale interessa molto di più i nostri amici a 4 zampe che si trovano facilmente tracciabili.

Un classico chip RFID è un circuito microscopico con un'antenna molto visibile. Se ne trovano facilmente sotto le etichette di CD e DVD oppure nei vestiti. Eviteranno i furti ma sono pericolosi per la nostra privacy.

:: Seguire il padrone

A meno di imbattersi in qualche cane miliardario, tipico delle leggende metropolitane in circolazione, la notizia è comunque di poco interesse. Probabilmente nessun cane se ne avrebbe mai a male se qualcuno seguisse tutte le sue mosse, anzi. La questione diventa di nostro interesse se pensiamo che quel cane non è da solo. Paola Barale non si separa mai dai suoi chihuahua, come Paris Hilton che porta il suo Thinkerbell dovunque. Lo stilista Valentino ha persino dedicato una collezione di abiti al suo amato cane Oliver e, come loro, migliaia di altre persone, famose o meno, vivono con almeno un cane e se lo portano con loro in continuazione. Risultato? Se è vero che tracciare una persona è difficile e illegale, tracciare il cane che sta con quella persona non solo risulta piuttosto semplice, visto che frequenze e caratteristiche dei chip canini sono note, ma addirittura non è certamente illegale. Il più delle volte, però, il risultato è lo stesso e con risvolti clamorosi come la possibilità di svolgere le intercettazioni alla luce del sole, visto che non si sta compiendo alcun reato. Tutto questo, sia chiaro, funziona perfettamente in via teorica ma finora non abbiamo avuto notizie di intercettazioni di questo genere. Non è detto, però, che in questo stesso istante non siano in corso operazioni di questo tipo. Pensandoci bene, credo che stasera rinuncerò alla passeggiata con l'amico 4 zampe. Non vorrei che qualche ladro abbia pensato queste cose e abbia deciso di tracciare le nostre passeggiate ai giardinetti mentre mi svuota la casa.

Un lettore di chip come quelli in dotazione ai veterinari. Funziona in modo semplice ed ha una potenza limitata, al punto da non mettere a rischio la privacy. Ma chi ci assicura che non possa essere sfruttato per altri scopi?

Controllare un cane con microchip è veloce e semplice. Peccato che questo chip serva a poco e possa creare qualche problema alla privacy del padrone.

Prosegue, ormai indistinta e per pochi spettatori, la Guerra dei Browser: ecco l'ultima battaglia

CHROME 2.0 VS. INTERNET EXPLORER 8

È passato poco tempo dal rilascio di Google Chrome nella versione beta 2 e Microsoft non si è fatta attendere, rispondendo con l'anticipo del rilascio di Internet Explorer 8. All'eterna versione beta dei prodotti Google siamo abituati, un poco meno a un anticipo da parte di Microsoft: vediamo che cosa abbiamo a disposizione con le nuove versioni di questi browser e se davvero vale la pena installarli sul nostro PC.

:: I vanti di Google

Quando Google ha presentato Chrome, la caratteristica principale su cui ha posto maggior rilevanza è stato il motore Javascript del browser, ritenuto il più veloce oggi disponibile. In effetti, le prove effettuate già con la prima beta di Chrome avevano evidenziato questa qualità, che sembra ancora migliorata nell'ultima release, addirittura si parla di un incremento delle prestazioni dell'ordine del 35%, un valore di tutto rispetto. Ma il problema non è certo l'aumento di prestazioni (ben venga!), piuttosto, i fattori da prendere in considerazione sono due: l'uso che se ne fa e l'instabilità delle versioni beta. Per quanto riguarda l'uso, molto dipende dai siti che si visitano più di frequente. Se siamo abituati a passare molto tempo su quelli che fanno ampio uso delle tecnologie Javascript, allora è facile che l'aumento di prestazioni sia sensibile: pensiamo per esempio ai molti giochi online che delegano

L'interfaccia di Chrome, semplice e piacevole, fa da contorno a un potente motore Javascript e al collaudato engine Webkit, utili nelle applicazioni Web di oggi come i giochi online che fanno ampio uso di script attivi.

ai client gran parte del lavoro di elaborazione, grafica o di programma, come Travian, OGame o simili, oppure alle numerose applicazioni cosiddette "Web 2.0", basate su AJAX e che spopolano specialmente nei siti di social networking. Nel caso di siti minimali, che comunque ancora oggi costituiscono una buona percentuale di quelli disponibili e visitabili in Rete, tutto questo vantaggio non è invece praticamente rilevabile, il classico esempio del tale che usa il SUV solo il sabato e la domenica per fare un giro in città.

Se fosse solo per questo, sarebbe anche una buona cosa installare Chrome. Ma qui viene la seconda nota dolente: questo benedetto incremento delle prestazioni è calcolato sulla versione unstable in fase di sviluppo paragonata alla versione stable che è quella normalmente scaricabile. Dovremo quindi scaricare una versione che presenterebbe tutti i problemi della classica release beta, cioè instabilità, possibili e frequenti crash, perdita di dati e così via. In sostanza, va bene installarla se vogliamo valutarlo e usarlo per fare un giro su Facebook, ma non ci fideremmo mai di compiere una transazione bancaria con Chrome beta unstable, almeno non finché le nuove caratteristiche non verranno rese disponibili anche nella versione beta stable.
Per il resto, Chrome non è un browser da disprezzare, ma non presenta alcuna novità eclatante. Ha le caratteristiche principali che oggi il pubblico richiede da ogni browser degno di questo nome, quali la navigazione a schede, la navigazione anonima (il cosiddetto "pornmode") e un'interfaccia piacevole e intuitiva, semplice da usare.

:: Le promesse di Microsoft

Internet Explorer 8 costituisce un'anomalia rispetto alla normale linea di condotta di Microsoft, per lo meno per quanto riguarda ciò che è successo negli ultimi anni. Innanzitutto, il periodo di beta è stato tutto sommato breve: l'uscita della versione definitiva ha addirittura anticipato i tempi, dato che nelle opinioni di Microsoft il prodotto era maturo per la pubblicazione finale. In secondo luogo, il periodo di "gestazione" della creatura è stato molto più breve di quello della versione precedente: solo due anni dal momento dell'uscita di Internet Explorer 7, mentre tra le versioni 6 e 7 sono passati ben 5 anni (lo stesso errore compiuto tra Windows XP e Vista, che in questo caso ha provocato una perdita dello share di utenza di IE di un buon 30% a vantaggio della concorrenza).
Le novità più significative per quanto riguarda IE 8 sono la velocità del renderer notevolmente migliorata, il modulo che "disegna" la pagina Web nella finestra del programma, che era sempre stato piuttosto scadente nelle versioni precedenti; gli Accelerator, cioè scorciatoie presenti nel menu contestuale della pagina visualizzata che rimandano a servizi offerti anche da terze parti (per esempio Google Maps) e che velocizzano l'operazione un tempo compiuta con il copia/incolla da un sito a un altro; infine, forse la novità più interessante, le Web Slice (tradotto letteralmente "fette di Web").

Internet Explorer 8 è molto simile, nella veste grafica, alla precedente versione. Interessante però l'implementazione delle Web Slice, porzioni di pagina che segnalano gli aggiornamenti, come questa proposta da Tuttovolume.it

Queste ultime sono porzioni di pagina Web che possono essere marcate per essere avvisati quando vengono aggiornate: iscrivendosi a una Web Slice questa apparirà in un'apposita barra del browser, in questo modo sarà possibile visualizzare solamente la porzione di pagina aggiornata e non tutto il documento. La cosa che meraviglia positivamente è che quest'ultima tecnologia sia stata rilasciata da Microsoft sotto una licenza Creative Commons: questo significa che anche altri browser potranno implementarla, e che potrebbe diventare presto un nuovo standard de facto.
Per quanto riguarda l'uso normale durante la navigazione, Internet Explorer si è limitato a riportare quanto già fatto in precedenza da altri browser, senza troppa infamia né lodi particolari. È quello che ci si aspettava e in questo tutto sommato Microsoft non ha deluso, ma a nostro avviso è troppo tardi perché questo permetta alla casa di Redmond di recuperare i punti persi negli anni precedenti a favore di altri browser come Firefox, Opera e Safari.

:: Quale browser?

Se siamo abituati a Firefox, per ora possiamo tranquillamente continuare a usarlo: nulla delle nuove versioni dei browser presentati lo farà rimpiangere. Tuttavia in questo periodo è bene tenere d'occhio attentamente cosa succede sul Web: Mozilla è parecchio indietro con la release di Firefox 3.5, le novità dei nuovi browser sono allettanti, e nulla è più facile che la tendenza sul Web sia l'implementazione più massiccia di Javascript e Web Slice.

La Wii è per giocare ma il Wiimote fa scintille se collegato al PC

Da Wiimote a mouse 3D

Lo scontro epocale tra Microsoft XBox e Sony PlayStation 3 si sta rivelando dannoso per entrambi i contendenti. Al di là degli aspetti puramente giocosi, la XBox risulta interessante per le possibilità di modding offerte mentre la PlayStation è tutt'ora il player di dischi BlueRay più economico sul mercato. A fare da terzo incomodo, quasi vincitore, c'è Nintendo, con la sua Wii. L'idea alla base del successo di questa consolle è che non serve avere una grafica troppo spinta o funzioni complesse per far divertire le persone. Visto che il gioco di maggior successo nella storia è il Tetris, la filosofia dichiarata da Nintendo è che l'indovinare meccaniche di gioco coinvolgenti vale più di qualsiasi capacità hardware. Da questo punto di vista, Nintendo sembra aver centrato l'obiettivo, presentando una consolle che elimina i classici controller in favore di un dispositivo senza fili e altamente sofisticato: il Wii Remote o Wiimote. D'altra parte, la resa grafica della Nintendo Wii è forse la più carente del mercato delle consolle di ultima generazione e per molti gamer si tratta di un handicap notevole. A fronte di giochi per PS3, XBox e PC con grafiche estremamente sofisticate e del tutto realistiche, quella della Wii sembra quasi una grafica datata. Il fascino del Wiimote, però, è notevole e l'esperienza di gioco a cui dà vita, fa passare quasi subito in secondo piano questo aspetto carente.

Un software come GlovePIE ci permette di creare gli script adatti ad ogni programma o gioco senza complicazioni particolari: basta curiosare tra gli innumerevoli esempi disponibili installati con il pacchetto.

:: Dalla Wii al PC

Con schede video capaci di risoluzioni elevatissime e schede audio che, ormai, arrivano normalmente a gestire 5.1 canali, se non addirittura 7.1, il PC è una piattaforma di gioco in piena concorrenza con PS3 e XBox che, però, non può nulla contro il sistema di gioco della Wii. L'ideale sarebbe poter coniugare la novità rappresentata dal

Con i suoi 11 tasti programmabili, il Wiimote è il candidato ideale al premio per il mouse più complesso mai creato prima. Grazie agli studi di design fatti da Nintendo, ha anche un uso molto semplice e intuitivo.

Usare gli strumenti della WII, consolle con una grafica apparentemente limitata, con giochi che sfruttano al massimo le meravigliose e potenti schede video per normali computer. Un fantastico binomio che ci farà sembrare preistorico ogni altro gioco.

Wiimote con la potenza grafica e sonora dei moderni computer. Un ideale che si può, per fortuna, raggiungere facilmente: il Wiimote si collega alla Wii tramite il sistema Bluetooth, uno standard anche in ambito PC. Naturalmente, Nintendo ha ottimizzato i collegamenti con la Wii e questo non permette un uso semplice del Wiimote con i computer: non sempre viene rilevato da tutti i dongle Bluetooth, molti Stack BT non lo sanno gestire, l'interfaccia con il sistema operativo è inesistente. A questo è comunque possibile porre facilmente un rimedio. Grazie all'opera di instancabili supporter, sono stati provati praticamente tutti i dongle Bluetooth sul mercato, in combinazione con tutti gli Stack BT disponibili, fino ad arrivare a identificare le combinazioni che permettono un collegamento sicuro del Wiimote a un sistema per cui non era progettato. Il software GlovePIE, originariamente concepito da Carl Kenner come sistema di gestione di input particolari, è stato poi adattato per il Wiimote. Il risultato è stato il collegamento sicuro e la possibilità di gestire totalmente il controller tramite un comune computer. Le implicazioni di questa combinazione sono esplosive. Non solo è possibile rinunciare al classico mouse in favore del Wiimote ma gli 11 tasti programmabili presenti su quest'ultimo permettono di coprire quasi tutte le esigenze per la gran parte dei giochi per PC, coniugando alla perfezione la potenza e la varietà dei giochi per PC con l'innovativo sistema di controllo della Wii. Il tutto senza essere costretti a comprare la consolle, visto che un Wiimote è in vendita a meno di 40 euro.

:: Si comincia

La prima cosa da fare è procurarsi un dongle Bluetooth da usare per il collegamento. In commercio ce

IL MOUSE 3D

Quando si parla di mouse vengono subito in mente i tappetini da abbinare: ad alta scorrevolezza, magari con qualche immagine piacevole. Sul mercato, tuttavia, hanno iniziato a diffondersi i mouse cosiddetti 3D, il cui utilizzo non è legato a una superficie particolare ma possono essere usati liberamente nell'aria, senza appoggi. Grazie ad una serie di accelerometri, dopo una calibrazione iniziale, questi dispositivi si rendono conto della loro posizione nello spazio 3D e permettono di controllare il cursore del mouse, un avatar in un gioco di ruolo, un aereo in un simulatore e via dicendo.

IL GIUSTO DONGLE

Anche se il Wiimote dispone di un collegamento Bluetooth motlo simile allo standard, è stato realizzato per essere usato esclusivamente con le Nintendo WII. Questo fa in modo che le sue capacità di collegamento siano ottimizzate per un hardware ben specifico e modifica il sistema di trasmissione rendendolo leggermente diverso dagli standard. Per ottenere i migliori collegamenti è opportuno utilizzare sistemi hardware che siano già stati testati con questo dispositivo. Gli accessori che rivelano una compatibilità maggiore sul maggior numero di computer sono i dongle Bluetooth della serie DBT prodotti dalla D-Link. Costano qualche decina di euro, funzionano benissimo come normali dongle ma hanno caratteristiche che li rendono particolarmente adatti al collegamento del Wiimote a qualsiasi computer.

ne sono moltissimi, con prezzi che vanno dai 10 ai 30 euro. Quelli che garantiscono migliori collegamenti sembrano essere quelli della serie DBT-12x, prodotti dalla DLink. In realtà, diversi dongle sul mercato sono perfettamente compatibili con il Wiimote ma occorre provarli uno alla volta per esserne sicuri. Una volta installato il nostro dongle e lo Stack Bluetooth a corredo, possiamo subito accendere il Wiimote e controllare che venga rilevato correttamente. In molti casi il rilevamento fallirà o verrà rilevata una periferica composita che lo Stack non riesce a gestire. Se è il nostro caso, possiamo provare a sostituire lo Stack del produttore con uno alternativo, a pagamento, come il BlueSoleil, prodotto dalla IVT. In alternativa, ma solo per 30 giorni, possiamo usare il BT Stack della Toshiba. Basta installarli come per qualsiasi altro programma e riprovare il collegamento: verrà riconosciuta, correttamente, una periferica HID RVL-CNT-01. Ora dobbiamo fare in modo che ai movimenti del Wiimote corrispondano delle azioni sul computer collegato. Questa operazione è possibile grazie al software GlovePIE, scaricabile dal sito http://carl.kenner.googlepages.com/glovepie. Estraiamo il file Zip, avviamo il programma nella cartella principale e avremo tutto il necessario per usare, finalmente, il Wiimote con il nostro PC.

:: Da programmare

Non è che avviando GlovePIE il cursore del mouse sia subito ai comandi del Wiimote: come tutti gli interpreti, GlovePIE va programmato correttamente. Il suo linguaggio di programmazione, però, è molto facile da comprendere e permette di fare moltissime cose, a nostro piacere. Per esempio, per recuperare il valore dell'accelerazione verticale si fa riferimento alla variabile Wiimote.RawForceX mentre per sapere se è stato premuto il pulsante A si fa riferimento alla variabile Wiimote.A.

CONCENTRATO DI TECNOLOGIA

Pensato come sistema di controllo innovativo rispetto agli standard del passato, il Wii remote, meglio noto come Wiimote, è un concentrato di tecnologie di altissimo livello. Dispone di accelerometri sui tre assi di movimento, in grado di indicare il posizionamento relativo dell'unità e l'indice di accelerazione in ogni direzione. A questo è abbinato un sistema a infrarossi che, con l'uso di una barra di sensori, permette di ottenere un miglioramento percettibile della precisione nello spazio 3D. A completamento dell'esperienza di gioco sono stati inseriti un altoparlante di limitata capacità e un sistema di feedback, chiamato rumble, per aumentare le sensazioni tattili del giocatore. Dal punto di vista delle capacità, contiene una memoria EEPROM da 16Kb, in cui 6Kb possono essere scritti e letti direttamente dalla WII e sono usati, per ora, per ospitare dati che possono essere così trasportati da una consolle all'altra senza l'uso di altri sistemi hardware. In più è disponibile una porta sul retro a cui collegare eventuali espansioni come il Nunchuk, una specie di estensione del Wiimote. A completamento del sistema ci sono 4 led integrati, comandabili via software, più 11 pulsanti completamente programmabili. Queste caratteristiche hanno fatto il successo della Wii ma limitare l'uso di uno strumento del genere al gioco puro è veramente uno spreco.

DAL WIIMOTE AL VR GLOVE

Carl Kenner poteva essere uno dei tanti programmatori sparsi per il mondo ma, qualche tempo fa, ha avuto un'idea geniale: vista la complessità del codice necessario per interfacciare Windows a sistemi alternativi ai mouse, ha dedicato molto del suo tempo allo sviluppo di un sistema che semplificasse la vita a utenti e programmatori. Dal suo lavoro è nato il Glove Programmable Input Emulator, meglio noto come GlovePIE. È un programma in grado di interpretare una serie di script che permettono di far corrispondere azioni di mouse e tastiera a input provenienti dalle fonti più svariate. Attualmente, GlovePIE supporta un hardware piuttosto ampio: sistemi eDimensional come TrackIR e SmartNav, tutti i joystick e gamepad riconosciuti da Windows, gamepad che usano la porta parallela, tutte le tastiere, mouse con più di 5 tasti e più di 2 assi di movimento, strumenti MIDI, microfoni, visori 3D e molto altro. Naturalmente supporta anche molti modelli di guanti di controllo 3D e il Wiimote. GlovePIE si può scaricare gratuitamente dal sito http://carl.kenner.googlepages.com/glovepie.

In questo modo, il Wiimote diventa un oggetto software che è possibile manipolare a piacimento con script che possono diventare anche molto complessi. Per agire sulla funzione che fa vibrare il Wiimote, per esempio, bisogna dare il comando Wiimote.Rumble = 1 mentre per spegnerla basta assegnargli il valore zero. Dal punto di vista strettamente sintattico, il linguaggio assomiglia molto al Visual Basic, pur non avendo molti costrutti. Possiamo giusto usare variabili, costanti, strutture if e poco altro. Il vantaggio è quello di avere un ambiente in cui non solo il Wiimote è considerato un banale oggetto ma anche altre caratteristiche tipiche di un PC sono virtualizzate come i comandi MIDI, il mouse, la tastiera e così via. In questo modo è possibile integrare il Wiimote non solo facendolo interagire con il puntatore del mouse ma facendo in modo che alla pressione di un tasto sul Wiimote corrisponda una certa sequenza di tasti premuti o l'esecuzione di un suono MIDI. In questo modo, con un po' di pratica, è possibile programmare il Wiimote per essere usato completamente con i normali giochi per PC: da quelli di corsa agli sparatutto, dagli sportivi agli strategici. In più possiamo farlo interagire anche con i normali programmi, agendo su PowerPoint per le nostre presentazioni oppure su Windows Media Player per usare il computer come impianto stereo. Le possibilità sono pressoché infinite e basta uno sguardo agli script di esempio forniti con GlovePIE per rendersi conto che l'unico limite è la nostra fantasia e capacità di combinare gli elementi a disposizione.

LO STACK BLUETOOTH

Ogni componente hardware del nostro computer deve disporre di un driver capace di farlo riconoscere al sistema operativo. Questa regola vale ancora di più per i dispositivi Bluetooth, in cui il driver non si limita a mettere in collegamento il sistema operativo con l'hardware ma include una serie di programmi indispensabili per il corretto funzionamento delle periferiche. Solitamente, questo driver composto, assume il nome di Stack Bluetooth e viene fornito dal produttore dell'hardware. In realtà, molti stack si assomigliano e con l'eccezione del driver vero e proprio, possono essere sostituiti facilmente tra loro. L'utilità di una sostituzione del genere sta nel fatto che ogni stack ha piccole differenze con gli altri. Alcuni hanno un sistema migliore di identificazione delle periferiche bluetooth, altri hanno una maggiore stabilità e via dicendo. Nel caso dei collegamenti tra computer e Wiimote, gli stack che si sono mostrati più affidabili sono quello prodotto dalla Toshiba, che si scarica dal sito aps2.toshiba-tro.de/bluetooth, e il BlueSoleil Stack prodotto dalla IVT, www.ivtcorporation.com. Purtroppo, il primo funziona solo per 30 giorni su sistemi diversi dai computer Toshiba, mentre il secondo è a pagamento. Nulla vieta, però, di provare altri Stack Bluetooth.

Dati che sfuggono, mercati in crisi, aziende in difficoltà e personaggi senza scrupoli. L'attuale trend graverà sulle aziende per anni

L'ARMADIO DELLE CHIAVI

Negli ultimi anni, l'informatica ha assunto un ruolo sempre più centrale nello sviluppo delle aziende. Ormai, nessuna azienda può fare a meno di avere a che fare con l'IT: che si tratti di un libero professionista con un computer o di una multinazionale che dispone di una rete geografica, il cuore di ogni azienda è costituita proprio dalla bistrattata (in Italia) struttura informativa. Questa diffusione, unita alla crisi che sta colpendo un po' tutti i settori, sta dando vita a fenomeni pericolosi.

:: Evoluzione

In funzione della diminuzione dei costi dovuta alle contrazioni di mercato, molte aziende cercano di liberarsi delle figure professionali più costose. In sostanza cercano di licenziare o spostare i lavoratori più esperti, visti spesso come semplici lavoratori anziani, acquisendo lavoratori di basso profilo che possano svolgere le stesse mansioni. In molti casi, questi bassi profili vengono semplicemente legati da contratti di collaborazione, evitando le assunzioni. In altri casi, addirittura, le funzioni vengono delegate in outsourcing: aziende esterne che si occupano di portare avanti il lavoro in sostituzione dei dipendenti. Dal punto di vista del mercato informatico, questa soluzione può essere molto valida ed è praticata da anni in campi specifici come la progettazione software, la gestione di siti Web e via dicendo. Unico campo che, fino a qualche tempo fa, faceva eccezione era quello dei Sistemi Informativi strettamente detti: gestione della LAN aziendale, assistenza agli utenti, gestione dei server, della connettività e via dicendo. Questo campo, direttamente a contatto con la struttura aziendale, era quasi sempre affidato a dipendenti. Ultimamente, invece, questo trend ha visto una brusca inversione: le aziende tendono a non acquistare più hardware, affittandolo, e ad affidare totalmente la sua gestione a società esterne di vario genere.

:: So come si fa

Se dal punto di vista dei costi si tratta di un fenomeno che permette di evitare un ricambio tecnologico continuo, permette di ridurre gli investimenti necessari e consente di abbattere i costi dovuti all'assunzione di figure professionali, ma dal punto di vista della sicurezza dell'azienda è uno dei peggiori autogol che si possa concepire. L'IT aziendale, a causa della sua centralità,

Il Documento Programmatico sulla Sicurezza è un obbligo di legge. In molti casi viene redatto dai commercialisti in sostituzione dei costosi amministratori IT, con risultati esilaranti.

La gestione delle policy permette a un amministratore di indicare come devono funzionare i client connessi alla rete LAN aziendale. Può limitare o ampliare i diritti degli utenti a suo piacere.

ha assunto sempre più una identità con l'azienda stessa. Sui server aziendali sono ospitati i conti della società, gli elenchi dei clienti, le mail, i contatti commerciali, i brevetti e chi più ne ha, più ne metta. Gli strumenti informatici di ogni azienda ospitano quello che viene definito know-how: il terzo pilastro su cui si regge l'azienda insieme alle persone e alle attrezzature. In molti casi, la scelta di ricorrere all'outsourcing viene fatta da dirigenti che non comprendono che, per sua natura intrinseca, un responsabile dell'IT non è solo il supervisore dell'hardware. I suoi interventi non si limitano a sostituire le parti hardware che si rovinano ma sono ben più numerosi in ambito software, per controllare i diritti degli utenti di accedere a una certa cartella riservata, sbloccare qualche programma che ha avuto un crash e così via. Tutte operazioni che un amministratore IT può fare con il suo account che è, per sua stessa definizione, di amministratore ed ha un potere sia fisico che logico sui contenuti della LAN. L'amministratore che gestisce il firewall può anche vedere chi si collega a Internet, quando lo fa e cosa fa. Esattamente come quando interviene per problemi di diritti su una cartella: per intervenire deve potervi accedere. Per le sue funzioni, l'amministratore di un sistema IT può entrare in qualsiasi computer collegato alla rete a patto che sia acceso e senza nemmeno che gli utenti se ne accorgano, può guardare nelle directory più segrete, può dare un'occhiata alla posta elettronica di ognuno, può recuperare la password di accesso di ogni singolo utente e fare molto altro. Per fare un paragone, l'amministratore di sistema è il custode di tutto e, proprio per questo, è colui che possiede la chiave che apre l'armadio delle chiavi. Quella che ricopre è una posizione di grave responsabilità: deve conoscere le leggi della sua professione, essere discreto, fedele all'azienda. Per questi motivi è spesso una figura costosa da mantenere.

A fronte di 1200 richieste delle aziende, nel database dei professionisti IT sono presenti oltre 65000 curriculum. Segnale di crisi ma anche di pericolo.

:: La barca affonda

Nell'attuale trend, gli amministratori tendono ad essere tra i primi a subire una sostituzione. Così, molte aziende riducono i costi e, in un colpo solo, ottengono due risultati importantissimi: regalano alla concorrenza una persona che sa tutto di come funziona l'azienda e la sostituiscono con altre che non hanno alcun interesse nella crescita aziendale.Non è un caso che l'offerta di acquisto di Yahoo da parte di Microsoft sia fallita non tanto per il prezzo, su cui si poteva trovare un accordo, ma perché i tecnici che hanno fatto la fortuna di Yahoo hanno minacciato di licenziarsi e fondare un'altra società o di passare a Google. Il futuro, si sa, non è prevedibile ma, se il trend non si invertirà, vedrà società svuotate di ogni know-how utile.

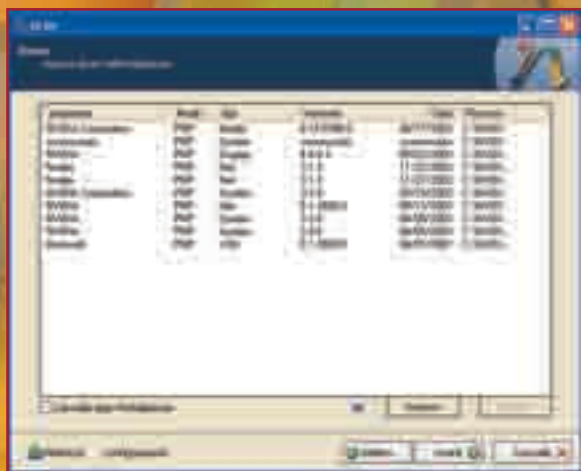
Costruiamo un DVD con la nostra installazione personalizzata

Setup ad hoc per Windows XP

Quando capita di dover reinstallare il sistema operativo e tutto il software sul PC ormai mettiamo sempre in conto che una buona giornata di lavoro se ne andrà ad aspettare che le procedure di installazione vengano completate. Una noia mortale, senza contare le volte in cui ci siamo dimenticati di fare il backup di particolari file di configurazione o non ci ricordiamo determinati parametri, come i numeri di serie, e ci perdiamo tra foglietti e appunti di vario genere alla ricerca di quelli corretti.
Anche per chi è puntiglioso al punto di scriversi accuratamente su un quaderno le procedure nella giusta sequenza, i tempi morti spesi aspettando che appaia la tal finestra per inserire un dato oppure di poter cambiare il CD per installare il programma successivo sono un tormento che si eviterebbe volentieri.
Non tutti lo sanno, ma con opportune manipolazioni dei file di installazione di Windows e di numerosi programmi è possibile costruire un DVD personalizzato che, in una volta sola, installi il sistema operativo e tutto il software che ci serve.

:: Slipstreaming

Il procedimento di installazione che si viene a creare si chiama slipstreaming, e non è difficile implementarlo se si conoscono alcuni trucchi.
Tutto parte dal presupposto che i software di installazione, compreso quello di Windows, basano le proprie operazioni su script che, opportunamente preparati in fase di confezionamento del prodotto, indicano al programma che operazione compiere secondo un ordine prestabilito. Tutto ciò che si compie, dalla creazione delle cartelle, alla decompressione e alla copia dei file, alla scrittura delle necessarie chiavi di registro e alla creazione dei collegamenti nel menu Avvio di Windows, è comandato da uno di questi script. Il programma di installazione può accettare anche dei comandi in ingresso, di solito nella forma *-comando* o */comando*, che possono essere impartiti lanciando l'eseguibile dal Prompt dei comandi e che influenzano lo svolgimento delle

La selezione delle operazioni da compiere in nLite.

In questa schermata possiamo includere i driver necessari per il nostro sistema. Ricordiamoci che i driver per il controller SATA vanno inseriti per primi!

operazioni successive. Usando questa possibilità, guidati da un apposito software, potremo creare un DVD avviabile personalizzato, contenente l'installazione di Windows XP, dei driver necessari ed eventualmente di altro software, come Office, Nero o, perché no, il nostro gioco preferito.

:: Che cosa ci serve

Innanzitutto dobbiamo procurarci il programma gratuito nLite: questo software, di cui abbiamo già parlato in altri numeri di HJ, consente di creare un'immagine ISO di Windows modificata secondo le nostre necessità. Il punto è che normalmente si pensa a ridurre al minimo il sistema operativo per togliere i fronzoli che non riteniamo necessari, mentre nLite permette anche di arricchirlo con altri elementi non disponibili con Windows stesso. Il primo di questi elementi che spesso è indispensabile includere per ottenere un'installazione che proceda da sola è il driver SATA per la nostra scheda madre. Lo standard SATA infatti è nato diverso tempo dopo l'uscita di Windows XP e non è presente nel CD originale di Microsoft. Alcuni di noi potrebbero avere una buona scheda madre che include questo driver nel BIOS, in tal caso l'installazione di Windows è trasparente, ma spesso, specialmente se il PC non è nuovissimo, i driver sono forniti a parte ed è sempre un gran mal di testa riuscire a installare il sistema operativo: viene richiesto il floppy con i driver, ma sui nuovi PC il lettore floppy non è più nella dotazione hardware! Procuriamoci poi tutti i file di installazione del software che intendiamo includere sul DVD: Office, Nero, Firefox o quello che sia, dopo il nostro lavoro saranno tutti sullo stesso supporto e potremo installarli senza dover cambiare disco ogni volta. Non potremo installarli contemporaneamente a Windows, ma almeno risparmieremo un po' di tempo (e in certi casi potremo automatizzare anche la loro installazione, come per Office).

:: Il solito nLite

Iniziamo copiando i file di installazione di Windows sull'hard disk, ci basta un semplice Copia/Incolla del contenuto del CD originale in una cartella dedicata. In altre cartelle sullo stesso disco decomprimiamo gli archivi che contengono i driver SATA e quelli dell'hardware del nostro PC, come scheda grafica, scheda di rete e driver audio. Non dimentichiamoci i driver USB, senza di questi probabilmente non riusciremo a usare le porte del PC secondo lo standard 2.0 e sfruttare tutta la velocità che questo permette. In un'altra cartella piazziamo anche i file contenenti i Service Pack di Windows. Teniamo presente che se vogliamo installare il SP 3 dovremo disporre almeno del SP 1, pertanto dovremo integrarne almeno due (il consiglio è integrare prima il SP 2 e poi il SP 3). nLite permette anche di integrare hotfixes pubblicate dopo l'ultimo Service Pack, ma possiamo anche farne a meno e installarle in seguito mediante gli aggiornamenti automatici del sistema. Avviamo quindi nLite e, dopo aver indicato dove si trovano i file di installazione di Windows, nella finestra delle opzioni attiviamo Service Pack, Driver, Informazioni Preinstallazione e ISO avviabile, che sono i diversi passaggi necessari per approntare il nostro setup personale. Iniziamo a integrare i Service Pack: la procedura è automatica, nLite decomprime i file scaricati da Microsoft autonomamente e li integra nei file di installazione del sistema. Integriamo prima il SP 2 e poi il SP3. Proseguiamo quindi con l'integrazione dei driver, iniziando dai SATA (che devono essere installati per primi) e continuando con gli altri. Assicuriamoci di installare i driver corretti per il nostro hardware. Per quanto riguarda le informazioni di preinstallazione, possiamo inserire il codice seriale di Windows perché non ci venga richiesto, configurare la rete, creare nuovi utenti, impostare il tema e altro ancora, secondo le nostre necessità.

Al termine, prima di creare la ISO, copiamo i file di installazione degli altri programmi che vogliamo includere nella cartella di lavoro: in questo modo, non appena avremo installato Windows, potremo procedere con la loro installazione. Per questo motivo è preferibile usare un DVD piuttosto di un semplice CD: avremo abbondante spazio a disposizione e non dovremo preoccuparci di cambiare supporto nel lettore del nostro computer. Più facile di così!

Alla fine si crea la ISO. Ci occorre un DVD se, per esempio, abbiamo incluso Office e altro software.

Tutto su uno dei più potenti Web scanner open source

NIKTO: IL RE DELLE SCANSIONI

Nella cassetta degli attrezzi di ogni hacker non può mancare un web scanner. Si tratta di un software in grado di fornirci preziose informazioni legate alla sicurezza di siti e servizi online. L'offerta in questo senso è molto buona, anche se dominata dai "soliti noti". Su tutti NMap. Tra le altre proposte, però, ne esiste una che gode di minor fama ma che non difetta certo in efficienza e velocità. Si tratta di Nikto Web Scanner, programma che concentra la sua tecnologia sulla ricerca di vulnerabilità nei software per server. Il suo funzionamento, a grandi linee, è piuttosto semplice: Nikto testa il servizio designato dall'utente, mettendolo a confronto il suo archivio interno, che comprende circa 3200 file ritenuti "pericolosi", le caratteristiche di oltre 900 tipi di webserver, e un lungo elenco di altri problemi noti (e meno noti).
Altra eccellente caratteristica di Nikto è di essere "open source": il suo codice è diffuso e modificato all'occorrenza da parte degli utenti più scaltri, tanto che ne è stata già realizzata una versione per Mac, chiamata (che originalità...) MacNikto.

:: Si basa sul Perl

L'utilizzo di Nikto non è propriamente materia adatta a chi è alle prime armi. Basti considerare che non è proposto con dei file binari, ma direttamente nel suo listato in linguaggio Perl. In realtà, superato lo shock iniziale, basta dotarsi di un apposito compilatore e il gioco è fatto. Venendo al dunque, per utilizzare Nikto, per prima cosa scarichiamolo da www.cirt.net/nikto2. Giunti a questa pagina, clicchiamo, sotto la sezione Download, su Version 2.03.gz (mentre leggiamo la versione potrebbe essere stata aggiornata). Il file in formato GZ è compresso: per estrarne il contenuto utilizziamo un programma freeware come ZipGenius (www.zipgenius.com). L'estrazione porta alla creazione, nel nostro disco fisso, della cartella principale Nikto (a meno che non ne abbiamo specificata una diversa). Al suo interno troviamo le sottocartelle .svn, docs, plugins e template, oltre ai file config.txt e quello principale, nikto.pl. All'interno di docs c'è l'eccellente manuale nikto_manual, in formato HTML. È fatto molto bene ed è indispensabile per un utilizzo approfondito del programma.

L'aggiornamento di Nikto non è frequente, ma avanza comunque per "blocchi" consistenti. La versione 2, già disponibile, è ricchissima di novità.

:: Ci vuole il compilatore

Oltre a Nikto, ci serve anche un compilatore Perl. Ce ne sono moltissimi a disposizione e all'indirizzo www.cpan.org troviamo di sicuro la versione che fa al caso nostro. Comunque, se utilizziamo Windows, una delle migliori soluzioni è ActivePerl, che scarichiamo gratuitamente da www.activestate.com/activeperl/. Una volta scaricato il file MSI, facciamoci sopra doppio clic sulla sua icona e poi su Esegui. Avviata la procedura d'installazione, clicchiamo su Next, spuntiamo la casella I accept the terms in the License Agreement, clicchiamo ancora su Next per tre volte e poi su Install. Al termine dell'installazione, togliamo il segno di spunta dalla casella Display the release notes e clicchiamo su Finish. Perl, di fatto, è installato nel nostro sistema e lo possiamo già utilizzare a riga di comando, dal DOS. A questo punto clicchiamo su Start, digitiamo cmd e premiamo Invio. Una volta in ambiente DOS, spostiamoci nella cartella Nikto e prepariamoci a utilizzare questo favoloso scanner (ovviamente dobbiamo essere collegati a Internet). La sintassi di base di Nikto è semplice:

perl nikto.pl -h 192.168.0.1

dove -h sta ad indicare che quello che segue è l'host da scansionare, mentre al posto di 192.168.0.1 dobbiamo specificare l'indirizzo IP desiderato. Possiamo ovviamente specificare anche una determinata porta per la scansione, col comando:

```
C:\nikto>ping www.google.com

Esecuzione di Ping www.l.google.com [74.125.43.99] con 32 byte di dati:

Risposta da 74.125.43.99: byte=32 durata=41ms TTL=241
Risposta da 74.125.43.99: byte=32 durata=40ms TTL=241
Risposta da 74.125.43.99: byte=32 durata=40ms TTL=241
Risposta da 74.125.43.99: byte=32 durata=40ms TTL=241

Statistiche Ping per 74.125.43.99:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 40ms, Massimo =  41ms, Medio =  40ms

C:\nikto>perl nikto.pl -h 74.125.43.99
- Nikto v2.03/2.04
---------------------------------------------------------------------------
+ Target IP:          74.125.43.99
+ Target Hostname:    bw-in-f99.google.com
+ Target Port:        80
+ Start Time:         2009-03-28 10:54:14
---------------------------------------------------------------------------
+ Server: gws
- /robots.txt - contains 167 'disallow' entries which should be manually viewed.
 (GET)
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-5737: WebLogic may reveal its internal IP or hostname in the Location he
ader. The value is "http://www.google.it/".
+ OSVDB-0: Non-standard header set-cookie returned by server, with contents: PRE
F=ID=5abbe7f20e84998f:TM=1238147868:LM=1238147868:S=G0d7ayMVl0vKcof0; expires=Su
n, 27-Mar-2011 09:57:48 GMT; path=/; domain=.google.com
+ OSVDB-0: GET /user.php?op=confirmnewuser&module=NS-NewUser&uname=%22%3E%3Cimg%
20src=%22javascript:alert(document.cookie);%22%3E&email=test@test.com : Post Nuk
e 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). http://www.cert.o
rg/advisories/CA-2000-02.html.
+ OSVDB-0: GET /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&ca
tegories=%3Cimg%20src=javascript:alert(document.cookie);%3E&parent_id=0 : Post N
uke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). http://www.cert
.org/advisories/CA-2000-02.html.
+ OSVDB-0: GET /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.
cookie);%3E&op=modload&name=Members_List&file=index : Post Nuke 0.7.2.3-Phoenix
is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2
000-02.html.
+ OSVDB-3092: GET /sitemap.xml : This gives a nice listing of the site content.
_
```

Un primo, veloce, controllo a un Web server di Google rivela alcune protezioni avanzate e non solo: abbiamo trovato anche qualche bella vulnerabilità.

perl nikto.pl -h 192.168.0.1 -p 443

dove -p indica che quello che segue è il numero di porta da controllare ("443" è un esempio che si riferisce alla porta TCP 443). Naturalmente, se di un sito conosciamo solo l'indirizzo URL, risaliamo al suo IP con il comando Ping. Buona parte dei firewall riconoscono le scansioni con Nikto (e non solo con lui) come veri e propri attacchi, e giocoforza le bloccano.

```
icrosoft Windows XP [Versione 5.1.2600]
C) Copyright 1985-2001 Microsoft Corp.

:\Documents and Settings\Max>ping www.google.com

secuzione di Ping www.google.com [74.125.39.106] con 32 byte di dati:

isposta da 74.125.39.106: byte=32 durata=55ms TTL=246
isposta da 74.125.39.106: byte=32 durata=54ms TTL=246
isposta da 74.125.39.106: byte=32 durata=53ms TTL=246
isposta da 74.125.39.106: byte=32 durata=54ms TTL=246

tatistiche Ping per 74.125.39.106:
  Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
empo approssimativo percorsi andata/ritorno in millisecondi:
  Minimo = 53ms, Massimo =  55ms, Medio =  54ms

:\Documents and Settings\Max>_
```

Andiamo a rompere le scatole a Google, pingando l'URL principale (www.google.com): otteniamo l'indirizzo IP del server corrispondente, proprio ciò che ci serviva.

In questo caso, vale la pena configurare il firewall per evitare questo genere di filtri, anche se così facendo ci esponiamo a molti rischi. Le informazioni elargite da Nikto sono a dir poco illuminanti. Se la scansione va a buon fine, infatti, otteniamo un rapporto che, per ogni hacker che si rispetti, è manna che cade dal cielo. Innanzitutto, vediamo il tipo di webserver utilizzato. A questa voce, seguono tutte le eventuali vulnerabilità rilevate o gli aggiornamenti mancanti. Per esempio, viene riportoto se la versione di Apache è vecchia (e dunque sensibile a bug noti), o se quella di PHP installata è in qualche modo "attaccabile". Ci sono anche informazioni sui moduli Perl e SSL, e in molti casi sono suggeriti metodi di exploit pronti all'uso. In questo articolo abbiamo solo scalfito le potenzialità di uno scanner che, a dispetto di una fama minore rispetto ai "colossi" del settore, offre un'efficienza senza eguali. Uno dei pochi difetti imputabili a Nikto è una certa lentezza, ampiamente ripagata, però, dalla quantità di informazioni elargite.

Impariamo gli standard di Internet leggendo i documenti con cui sono nati

REQUEST FOR COMMENTS

Il desiderio di capire nei più intimi dettagli il funzionamento di qualsiasi apparecchiatura è una delle caratteristiche tipiche dell'hacker. Da questo punto di vista Internet rappresenta uno degli oggetti di studio più entusiasmanti, in quanto offre un'enorme varietà di concetti da imparare: basti pensare a quanti sono i formati e gli standard su cui si basa... E a quanti simpatici hack potremmo fare una volta compreso il loro funzionamento più profondo!

La maggior parte di questi standard è pubblicata in documenti liberamente accessibili e facili da reperire: si chiamano RFC (Request For Comments) e vengono utilizzati da ormai quarant'anni per condividere informazioni e osservazioni relative a formati, standard, protocolli e tecnologie di Internet. La prima RFC risale infatti al 1969 e da allora ne sono state pubblicate più di 5500. Ognuna di esse supera un complicato processo di selezione da parte di un organismo chiamato IETF (Internet Engineering Task Force), il cui compito è "far sì che Internet funzioni nel modo migliore possibile".

:: Il formato delle RFC

Per diventare RFC, un documento tecnico deve innanzitutto seguire uno standard ben preciso: un semplice file di testo a 73 colonne, formattato esclusivamente con caratteri ASCII standard. Perché questa scelta? Semplice: quale formato, infatti, è rimasto invariato dal 1969 ad oggi e può essere visualizzato su un qualsiasi computer, indipendentemente da quanto sia vecchio e da che sistema operativo usi?

Ogni RFC presenta un'intestazione che contiene informazioni particolarmente utili per il lettore. Oltre a titolo,

John Postel, uno degli autori della prima RFC e partecipante attivo al progetto per 28 anni, ha sempre usato tastiera con solo due dita!

data e autori, infatti, compaiono anche il numero identificativo del documento, le relazioni con documenti precedenti e la categoria di appartenenza. Per esempio, l'RFC più recente che descrive il protocollo SMTP è la 5321, che aggiorna l'RFC 1123, rende obsoleta la 2821 e appartiene alla categoria chiamata "Standards Track".
Le categorie a cui una RFC può appartenere sono diverse; i documenti che possono essere considerati più ufficiali sono divisi in tre categorie principali: gli standard ormai consolidati (standard), le bozze (draft) e le proposte di standard (proposed). Vi sono poi tre classi non standard che comprendono i documenti sperimentali (experimental), quelli informativi (informational) e quelli storici (historic). C'è poi una categoria che potremmo definire "quasi standard" che contiene le Best Current Practice (BCP), cioè tutte quelle pratiche non ancora ufficiali ma che vengono considerate le più logiche da adottare.

:: Trovare il documento che cerchiamo

Ora che sappiamo comprendere il significato dei metadati associati a una RFC, non ci resta che sbirciare all'interno dell'archivio ufficiale dell'IETF per vedere se ci sono delle informazioni che possono interessarci.
Ci sono diversi metodi: il primo, e più semplice, può essere usato quando conosciamo il numero identificativo del documento e consiste nel collegarsi all'indirizzo http://www.ietf.org/rfc/rfcxxxx.txt, dove xxxx corrisponde all'identificativo. Per esempio, la prima RFC della storia si trova all'indirizzo http://www.ietf.org/rfc/rfc0001.txt.
Un altro metodo di ricerca consiste nel partire dal nome del protocollo a cui siamo interessati e cercare tutti i documenti che lo riguardano. Per questo scopo possiamo utilizzare l'elenco degli Official Internet Protocol Standards che si trova all'indirizzo http://www.rfc-editor.org/rfcxx00.html: per esempio, i protocolli IP, ICMP ed IGMP sono descritti in RFC diverse ma fanno tutti parte dello stesso standard numero 5. Infine possiamo cercare i documenti in base al loro stato o categoria di appartenenza: all'indirizzo http://www.rfc-editor.org/category.html è pubblicato l'indice delle RFC suddiviso in base allo stato di pubblicazione e, per ogni sezione, i documenti aggiornati compaiono in nero mentre quelli obsoleti compaiono in rosso, insieme al numero identificativo delle RFC che li hanno sostituiti.

Nonostante diversi standard siano ormai più che consolidati, il numero di RFC pubblicate è sempre in aumento.

Gli strumenti appena descritti dovrebbero esserci più che sufficienti nella maggior parte dei casi: solitamente, infatti, conosciamo almeno il nome del protocollo che desideriamo studiare, se non addirittura il codice dell'RFC all'interno del quale è descritto. Tuttavia, nel caso in cui abbiamo solo una vaga idea dei concetti che desideriamo approfondire, possiamo utilizzare il motore di ricerca messo a disposizione all'indirizzo http://www.rfc-editor.org/rfcsearch.html. Se, per esempio, desideriamo conoscere come vengono codificati gli allegati all'interno dei messaggi di posta elettronica, possiamo cercare "mail attachment" e ottenere come risultato i titoli delle RFC che trattano specificatamente quest'argomento (nella fattispecie, l'RFC 2183).

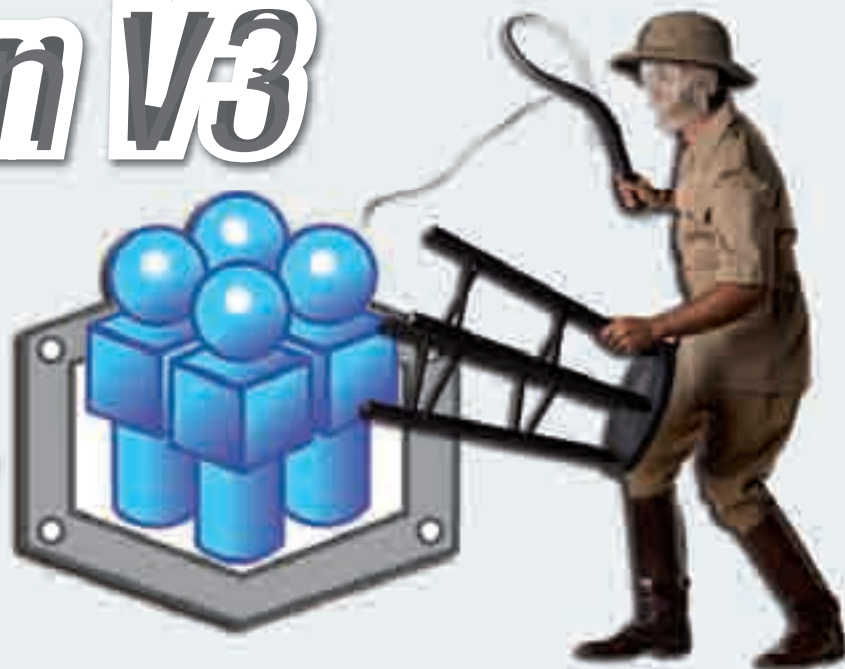
```
Network Working Group                                   J. Klensin
Request for Comments: 5321                            October 2008
Obsoletes: 2821
Updates: 1123
Category: Standards Track

                 Simple Mail Transfer Protocol
```

L'intestazione della RFC 5321, il documento dedicato al protocollo SMTP.

:: Cosa possiamo leggere ora?

Il problema più grosso quando ci si confronta con un archivio di queste dimensioni è l'enorme quantità di informazioni a disposizione: una sola vita non ci basterà per leggere tutte le RFC!
Se non sappiamo da dove cominciare possiamo partire da quelli più semplici, come per esempio quelli relativi alla posta elettronica (POP3, IMAP e SMTP), al Web (HTTP) o agli altri più diffusi protocolli a livello di applicazione (FTP, IRC, DNS e così via). I protocolli a livello di trasporto e di rete, come TCP e IP, sono decisamente più complicati ma non per questo meno interessanti.
Una menzione a parte la meritano i documenti pubblicati il primo di aprile, in quanto pur rispettando l'aspetto formale delle RFC sono il più delle volte delle divertenti bufale (http://en.wikipedia.org/wiki/April_Fools%27_Day_RFC).
Infine, se abbiamo ancora qualche difficoltà con l'inglese possiamo trovare delle traduzioni italiane delle RFC più comuni all'indirizzo http://rfc.altervista.org, un progetto collaborativo (e sempre aperto a molteplici contributi!) che rispecchia la mentalità hacker di rendere le informazioni accessibili al maggior numero possibile di persone.

Addomestichiamo Symbian V3

Come installare applicazioni non ufficiali sul nostro cellulare

Hai appena comprato un fiammante telefonino con una delle ultime versioni di Symbian, inizi a scaricare un po' di applicazioni non proprio ufficiali e il cellulare si rifiuta di installarle perché l'applicazione "non ha un certificato valido". E inoltre non è possibile accedere alle cartelle di sistema, come mai?
Nokia ha inserito nelle ultime versioni dei suoi smartphone una protezione legata alla certificazione delle applicazioni che ha lo scopo principale di permettere l'installazione solo di software controllato, ufficialmente dalla community, ma sostanzialmente proprio dalla casa finlandese; pratica che può limitare l'uso del telefono a ciò che è loro più conveniente. Questa politica ovviamente non ci piace e in molti hanno studiato diversi metodi per addomesticare questi firmware poco amichevoli.
Va premesso che queste procedure, anche nel caso in cui non compromettano il firmware a bordo del telefono, sono al limite dell'invalidazione della garanzia; nel caso si volesse tornare indietro è consigliabile quindi effettuare un "deep reset" del cellulare che lo riporti alle impostazioni di fabbrica con il comando *#7370# impartito in modalità base, ma non è escluso che possa occorrere un ripristino completo del firmware nel caso i file aggiunti non vengano comunque rimossi.

:: Il metodo di FCA00000

Tra i diversi metodi disponibili illustriamo di seguito la procedura abbastanza semplice e poco invasiva messa a punto da un simpatico hacker, che si è soprannominato FCA00000.
Come cavia abbiamo utilizzato un E51 con la versione del firmware di ottobre 2008, nonostante la procedura non fosse garantita per i firmware successivi a luglio 2008. Tutti i software sono facilmente recuperabili in rete e in particolare, oltre al telefonino con Symbian V3, Nokia PC Suite (ultima versione) e il cavo dati in dotazione per il trasferimento delle applicazioni, ci occorrono:

- Hello Carbide
- CapsON e CapsOFF (da scompattare sul PC) che contengono al loro interno anche il file CProfDriver_SISX.ldd da scegliere della versione opportuna per il proprio telefono (vedi BOX); una volta individuato copiarlo in una cartella temporanea del telefono o sulla sua memoria esterna perché ci servirà più avanti:
- X-plore
- InstallServer

A parte X-plore, gli altri software sono

▲ *Il Nokia E51 come molti altri modelli monta Symbian V3 e presenta delle protezioni d'accesso alle cartelle di sistema inserite nel firmware.*

Figura 1. Va bene una versione qualsiasi di X-plore, shareware scaricabile da http://www.lonelygames.com. Il programma è ben fatto, ma ci sono diverse alternative.

gratuiti. X-plore è shareware e dato che va utilizzato solo nella fase iniziale, se non lo si vuole acquistare in seguito lo si può tranquillamente disinstallare una volta terminata la procedura.

Figura 2. Una volta installato, Hello Carbide comparirà nel menu, ma non dobbiamo ancora lanciarlo. Ci servirà dopo per superare la protezione del firmware.

:: Hack permanente

Come primo passo dobbiamo permettere l'installazione di applicazioni non certificate; andiamo quindi in Menu→ Installazioni→ Gestione applicazioni→ Opzioni→ Impostazioni→ Installazione software e selezioniamo Completa (di default c'è il blocco per applicazioni non firmate).
A questo punto siamo pronti per l'hack. Installiamo e lanciamo X-plore e in TOOLS→CONFIGURATION spuntiamo le prime 4 caselle quadrate; poi chiudiamo l'applicazione (vedi **Figura 1**). Installiamo Hello Carbide, senza poi lanciarlo (vedi **Figura 2**).
Riapriamo X-plore e lasciamolo in background (per esempio premendo il tasto per aprire il menu di sistema).
Ora lanciamo Hello Carbide, selezioniamo OPZIONI poi MENU1 e per ogni messaggio che comparirà selezioniamo sempre Sì (Yes), finché l'applicazione non va in crash (solitamente dopo aver visualizzato il messaggio "done... probably", vedi **Figura 3**).

In questo momento il sistema è instabile, ma X-plore è ancora perfettamente in esecuzione e le cartelle di sistema sono scrivibili! Tramite X-plore spostiamo quindi il file CProfDriver_SISX.ldd dalla cartella temporanea in C:\sys\bin e riavviamo il nostro telefonino.
Al riavvio installiamo i file .sis di CapsON e di CapsOFF che permetteranno rispettivamente di abilitare o disabilitare la protezione sulle cartelle di sistema; l'hack sarà già operativo!
Ora possiamo allargare l'hack per installare qualunque tipo di file UNSIGNED tramite installserver.exe che andrà copiato sempre in C:\sys\bin (cui possiamo tranquillamente accedere dopo aver lanciato CapsOFF).

Una volta resi operativi installserver, CapsON e CapsOFF, possiamo disinstallare Hello Carbide e divertirci a provare qualunque applicazione, che certificata o no da Symbian. Non solo: potendo ora accedere liberamente alle cartelle di sistema è anche possibile effettuare alcuni modding del nostro telefonino Symbian, come il cambio del suono allo startup (vedi www.nokioteca.net/home/forum/index.php?showtopic=116080) o la

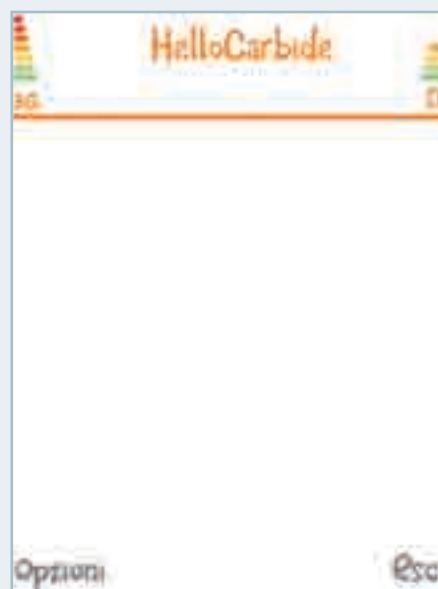



Figura 3. Non diamo peso ai messaggi visualizzati nei box e andiamo avanti cliccando sempre Sì (Yes) finché Hello Carbide si chiude da solo (per crash).

rimozione di animazioni in accensione e spegnimento senza sostituzione o modifica del firmware (vedi www.nokioteca.net/home/forum/index.php?showtopic=116095).

Massimiliano Brasile

DOVE FUNZIONA

SymbianOS 9.1:
prendere "preFP1_CapsOnOff" per telefonini Pre-FP1 (3250 - 5500 - 6290 - E50 - E60 - E61 - E61i - E62 - E65 - E70 - N71 - N73 - N75 - N77 - N80 - N91 - N92 - N93 – N93i).

SymbianOS 9.2:
prendere "FP1_CapsOnOff" per telefonini FP1 (5700 - 6110 Navigator - 6120 - 6121 - 6290 - E51 - E90 - N76 - N81 - N81 8Gb - N82 - N95 - N95 8Gb - N78 e N79).

Scegliere il file CprofDriver_SISX.ldd opportuno in base al cellulare sul quale si va ad operare.